Nebelkerzen zur Online-Durchsuchung

Der Kaiser ist bekanntlich nackt und Online-Durchsuchungen hat es nie gegeben und wird es nie geben. Jedenfalls nicht so, wie sie der Volksmund und Klein Wolfgang verstehen: Da sitzt ein Ermittler irgendwo in einer Behörde und sucht und findet die IP-Adresse des Computers eines Verdächtigen, spielt dem dann „online“ und unbemerkt ein Spionageprogramm auf und liest dann mit? Vergesst es. Keep on dreaming. Die real gar nicht existierende Online-Durchsuchung ist der einflussreichste Medien-Hoax, den ich kenne, ein hübsches urbanes Märchen, das vom Wünschen und Wollen ahnungsloser internet-Ausdrucker und noch mehr vom ahnungslosen Geraune der Medien am Leben erhalten wird. Nicht *ich* muss beweisen, dass es bisher *keine* „Online-Durchsuchung gab, sondern diejenigem, die behaupten, so etwas würde gemacht, müssen Fakten, Fakten, Fakten liefern – wer, wie und womit. Eine Presseerklärung irgendeines Innenministeriums gilt nicht als Beweis.

Der Deutschlandfunk hat jetzt eine schöne Nebelkerze geworfen: Man interviewte Peter Welchering, den FDP-Stadtverbandsvorsitzender und Kreisvorsitzender des DJV zum Thema. (Für Insider: Welchering und Karl Geibel sind in

demselben DJV-Verband.) Ach ja, Journalist ist Welchering auch noch und Erfinder des Tron-Netzes.

Sorry, aber ich vergesse nie etwas – Originalton Welchering in einem Artikel vor zwei Jahren: „Wird eine verschlüsselte Datei einmal auf die Festplatte eines Internet-Rechners kopiert, ist sie – auch wenn sie sofort danach wieder gelöscht wird – mit einigem Aufwand mittels Online-Durchsuchung für Datenspione sichtbar.“ Der gute Mann hat also keinen blassen Schimmer.

[Irrelevanter Einschub: Und deshalb war Welchering vermutlich der einzige Journalist, der versuchte, im MediumMagazin die PrivacyBox zu diskreditieren. Er meinte mich, prügelte aber auf die Privacybox ein. So funktioniert Mobbing im DJV. Ich habe ja seinen geliebten Großen Vorsitzenden Charly Geibel ständig angegriffen und der Unfähgkeit bezichtigt. Das tut man nicht unter Journalistenfunktionären. Und ausserdem war ich Chefredakteur von Berliner Journalisten, dem einzig ernst zu nehmenden Konkurrenten des MediumMagazins. Aber ich schweife ab…]

Irgendwie haben sie es ja gemerkt, dass es mit der Online-Durchsuchung nicht so weit her ist. Ja, wo durchsuchen sie denn? Manfred Kloiber fragt: „Welche technischen Probleme machen denn den BKA-Beamten das Leben schwer, Peter Welchering?“ Man muss sich die Anwort auf der Zunge zergehen lassen: „Denn diese Firewall, die verhindert, dass der sogenannte Infiltrationsschädling eindringen kann, das ist im wesentlichen ein Downloader, ein Trojaner, der sich ins System schleicht, um das eigentliche Überwachungsmodul, auf die es ja den Ermittlern ankommt, das dann auch die eigentliche Durchsuchungssoftware von einem BKA-Server herunterladen soll. Das ist insofern etwas verwunderlich, als die von den Geheimdiensten eingesetzten Bundestrojaner dieses Problem eigentlich schon gelöst hatten, und das schon vor einigen

Jahren.“ 

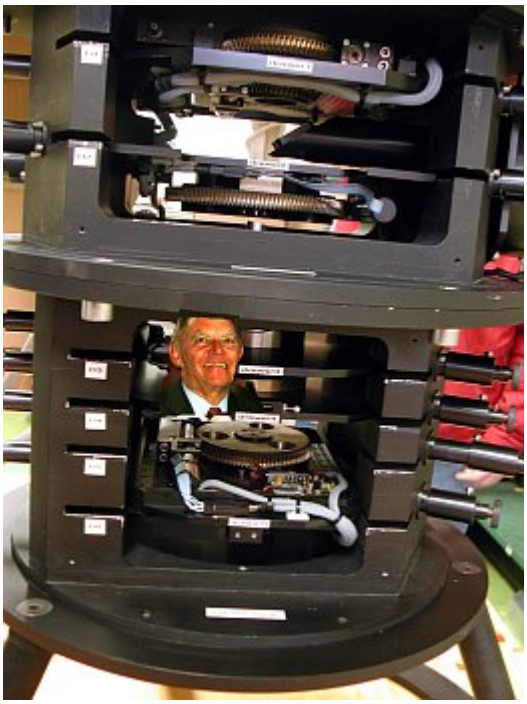
Ja, sie hatten „das Problem“ schon gelöst? Gibt es dazu vielleicht irgendeine winzige Tatsache, die aus einer unabhängigen Quelle stammt? Nein, gar nicht. Null. Es ist nur vages Gefasel. Und: Woher will Welchering das wissen? „Nach allem, was man aus den so schüchternen Sicherheitskreisen so hört“ – das ist. mit Verlaub und meiner Meinung nach pure Aufschneiderei. Mit „Sicherheitskreisen“ meinen Journalisten in der Regel die Presseabteilungen der Verfassungsschützer. Und die sind so seriös wie der ehemalige irakische Informationsminister.

Welchering behauptet allen Ernstes, der Bundesnachrichtendienst habe „solche Angriffsprogramme aus mehr oder weniger gut getarnten Quellen beschafft.“ Woher weiß er das? Das weiß ich wiederum: Von Focus Online, die das ständig mit wachsender Begeisterung, aber faktenfrei behaupten. Oder von Spiegel Online vom Frühjahr 2009: „Nach Informationen des SPIEGEL hat der Geheimdienst BND in den vergangenen Jahren in mindestens 2500 Fällen PCs im Ausland durchsucht“. Aber nicht „online“, sondern Keylogger physikalisch installiert und/oder schlicht die E-Mail-Accounts abgerufen wie beim afghanischen Handelsminister. Welchering weiß nicht mehr, als das, was in der Zeitung steht.

Jetzt fragt Kloiber: „Letztlich handelt es sich ja auch beim Bundestrojaner um ein Computervirus. Und deren Ausbreitung ist ja nicht völlig unter Kontrolle zu halten.“ Nonsens und Schwachfug, wie Wau Holland es funktioniert hätte. Jetzt ist der „Trojaner“ also ein „Virus“? Eine Lokomoive ist also irgendwie ein Auto, und das Usenet ist dasselbe wie das Word Wide Web, und ein Kamel ist auch irgendwie in Pferd? Wenn man etwas nicht kontrollieren kann, dann ist es

ermittlungstechnisch -und taktisch ohnehin Quatsch, von der Beweiskraft vor Gericht ganz zu schweigen.

Welcherung: „Offenbar war man in Wiesbaden mit den Parameterermittlungen, die es ja auch kommerziell zu kaufen gibt, nicht so übermäßig zufrieden. Und man hat deshalb einen anderen Weg eingeschlagen, solche Systemparameter auszuspähen, aber der ist auch nicht erfolgreich gewesen, der ist von den Betriebssystemherstellern dichtgemacht worden. Das funktioniert recht elegant. Die Ermittler haben einfach ein Sicherheitsupdate eines Betriebssystemherstellers genommen und dem einen Trojaner angehängt. Weil Sicherheitsupdates ja automatisch heruntergeladen werden, bemerken die Überwachten PC-Besitzer das gar nicht.“ Ach ja? Gibt es dafür Quellen? Nein, gibt es nicht. Welcherung ist der einzige Mensch auf der Welt, der davon weiß. Er weiß mehr als der Chaos Computer Club und die c’t zusammen. Vielleicht ist das der Grund, warum er in der FDP ist… Da sind ausschließlich solche klugen Menschen.



„Kloiber: Welche Strategien werden denn derzeit im BKA favorisiert, um die technischen Schwierigkeiten beim Einsatz des Bundestrojaners zu überwinden?
Welchering: Das ist schwierig zu ermitteln. Auf solche Fragen schweigt das BKA natürlich“.

Eben. Nichts Genaues weiß man nicht. Man weiß überhaupt nichts, auch nichts über Exploits, mit denen das laut Welchering angeblich gemacht wird. Um so lauter tönen diejenigen, die die magische Online-Durchsuchung herbeifantasieren wollen. irgendwie erinnert mich das geheimisvolle Getöne an Voodoo und Regenzauber. Irgendwelche obskuren Männer stehen im Kreis oder im Viereck und murmeln etwas gemeinsam, auf das die Welt so sei, wie sie es wünschen.

By the way: Wenn ihr das Buch nicht lesen wollt, dann lest die Artikel, die ich 2007 zum Thema gebloggt habe. Har har.

spiggel.de (07.02.2007): „Der Staats-Trojaner-Hoax“
spiggel.de (08.02.2007): „Der Staats-Trojaner-Hoax, update“
spiggel.de (09.02.2007): „Wie schütze ich mich vor dem Bundestrojaner?“
spiggel.de (11.02.2007): „Der SPIEGEL heizt den Hoax an“
spiggel.de (13.02.2007): „Jetzt ganz neu: Social Engineering“
spiggel.de (12.03.2007): „Online-Durchsuchungen, die 234te“
spiggel.de (18.03.2007): „Online-Kriminelle immer onliner und immer krimineller“
spiggel.de (07.04.2007): „Online-Durchsuchungen: Die Farce geht weiter“
spiggel.de (28.04.2007): „Schäuble ist nackt“
spiggel.de (06.05.2007): „Auch du, meine Christiane?“
spiggel.de (10.05.2007): „Der Koran, geile Titten und der Quelle-Katalog“
spiggel.de (10.05.2007): „Heimlicher Zugriff auf IT-Systeme“
spiggel.de (19.05.2007): „Online-Duchsuchung in Second Life!“
spiggel.de (30.06.2007): „Wie tötet man eine Online-Ente?“
spiggel.de (01.07.2007): „Digitale Spaltung?“
spiggel.de (08.07.2007): „Sex-Verbot für Terroristen?“
spiggel.de (12.07.2007): „Wie Enten geklont werden“
spiggel.de (15.07.2007): „Richter erklärt die Online-Durchsuchung zur Ente“
spiggel.de (19.07.2007): „Heise Hoax-verseucht“
spiggel.de (31.07.2007): „Hurra, so funktionieren Online-

Durchsuchungen!“
spiggel.de (25.08.2007): „Sie haben ein Attachment bekommen“
spiggel.de (28.08.2007): „Blauäugige Keylogger“
spiggel.de (30.08.2007): „Gefälschte Behörden-E-Mails?“
spiggel.de (03.10.2007): „Keine Chance für Online-Durchsuchung“
spiggel.de (07.10.2007): „Das Märchen vom Datenstrom“
spiggel.de (22.10.2007): „Technische Details offen“
spiggel.de (10.11.2007): „Neues vom Tron-Netz“
spiggel.de (13.11.2007): „Eintagstrojaner mit Verfallsdatum“
spiggel.de (10.11.2007): „Zierckes Traum“
spiggel.de (19.11.2007): „Terroristen nutzen Windows“
spiggel.de (16.12.2007): „HTTP 909 – Bundestrojaner-Online-Durchsuchung“